MR2833-34

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants:	Laurent Eschenauer, et al.	:	Group
Serial No:	10/666,207	:	Art Unit #2877
Filed:	18 September 2003	:	Examiner
Title:	METHOD AND APPARATUS FOR KEY MANAGEMENT IN DISTRIBUTED SENSOR NETWORKS	:	Unknown

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT

Honorable Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

The Applicants wish to make the following art references of record in the above-identified Patent Application pursuant to 37 C.F.R. §§ 1.97 and 1.98, and to the Duty of Disclosure set forth in 37 C.F.R. § 1.56.

Although the information submitted herewith may be "material" to the Examiner's consideration of the subject Patent Application, this submission is not intended to constitute an admission that such information is "prior art" as to the claimed invention.

In accordance with 37 C.F.R. § 1.97(g), the filing of this Supplemental Information Disclosure Statement shall not be construed to mean that a search was made or that no other material information, as defined in 37 C.F.R. § 1.56(b), exists.

Cited Publications are:

Ref. No.	Description
B1	C. Blundo, A. DeSantis, A. Herzberg, S. Kutten, U. Vaccaro and M. Yung, "Perfectly Secure Key Distribution for Dynamic Conferences," in Advances in Cryptology - CRYPTO '92, LNCS 740, Springer –Verlag, Berlin, August 1993, pp. 471-486.
C1	C. Blundo, L.A. Frota Mattos and D.R. Stinson, "Tradeoffs Between Communication and Storage in Unconditionally Secure Schemes for Broadcast Encryption and Interactive Key Distribution,: Advances in Cryptology – CRYPTO '96, LNCS 1109, Springer Verlag, Berlin, August 1996, pp. 387-400.
D1	A. Fiat and M. Naor, "Broadcast Encryption," in Advances in Cryptology – CRYPTO '93, LNCS 773, Springer-Verlag, Berlin, August 1993, pp. 480-491.
E1	J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler, K. Pister, "System architecture directions for network sensor," Proc. Of ASPLOS-IX, Cambridge, Mass. 2000.
F1	V.D. Gligor and P. Donescu, "Fast Encryption and Authentication: XCBC Encryption and XECB Authentication Modes, " Fast Software Encryption 2001, M. Matsui (ed), LNCS 2355, Springer Verlag, April 2001.
G1	C.S. Jutla, "Encryption Modes with Almost Free Message Integrity," Advances in Cryptology – EUROCRYPT 2001, B. Pfitzmann (ed.), LNCS 2045, Springer Verlag, May 2001.
H1	J.M. Kahn, R.H. Katz and K.S.J. Pister, "Mobile Networking for Smart Dust," ACM/IEEE Intl. Conf. on Mobile Computing and Networking (MobiCom 99), Seattle, WA, August 17-19, 1999, pp. 271-278.
I1	P. Rogaway, M. Bellare, J. Black, and T. Krovetz, "OCB: A block-Cipher Mode of Operations for Efficient Authenticated Encryption," Proc. of the 8th ACM Conf. on Computer and Communication Security, Philadelphia, Penn., November 2001.

J1 S.R. White and L. Comerford, "ABYSS: An Architecture for Software Protection," IEEE Transactions on Software Engineering, vol. 16, No. 6, June 1990, pp. 619-629.

This Supplemental Information Disclosure Statement is being filed more than three months subsequent to the Filing Date of the subject Patent Application, but before the mailing of a first Office Action.

A Form PTO-1449 and copies of the references are submitted along with this document. It is requested that the Examiner consider the references and make them of record in the above-referenced Patent Application.

Respectfully submitted,
FOR: ROSENBERG, KLEIN & LEE

David I. Klein
Registration #33,253

Dated: 20 Aug. 2004

Suite 101
3458 Ellicott Center Drive
Ellicott City, MD 21043
(410) 465-6678

PTO/SB/08B (08-03)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 1

Complete if Known	
Application Number	10/666,207
Filing Date	18 SEPTEMBER 2003
First Named Inventor	LAURENT ESCHENAUER
Art Unit	2877
Examiner Name	UNKNOWN
Attorney Docket Number	MR2833-34

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
	B1	C. Blundo, A. DeSantis, A. Herzberg, S. Kutten, U. Vaccaro and M. Yung, "Perfectly Secure Key Distribution for Dynamic Conferences," in Advances in Cryptology - CRYPTO	
	C1	C. Blundo, L.A. Frota Mattos and D.R. Stinson, "Tradeoffs Between Communication and Storage in Unconditionally Secure Schemes for Broadcast Encryption and Interactive K	
	D1	A. Fiat and M. Naor, "Broadcast Encryption," in Advances in Cryptology – CRYPTO '93, LNCS 773, Springer-Verlag, Berlin, August 1993, pp. 480- 491.	
	E1	J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler, K. Pister, "System architecture directions for network sensor," Proc. Of ASPLOS-IX, Cambridge, Mass. 2000.	
	F1	V.D. Gligor and P. Donescu, "Fast Encryption and Authentication: XCBC Encryption and XECB Authentication Modes, " Fast Software Encryption 2001, M. Matsui (ed), LNCS 235	
	G1	C.S. Jutla, "Encryption Modes with Almost Free Message Integrity," Advances in Cryptology – EUROCRYPT 2001, B. Pfitzmann (ed.), LNCS 2045, Springer Verlag, May 2001.	
	H1	J.M. Kahn, R.H. Katz and K.S.J. Pister, "Mobile Networking for Smart Dust," ACM/IEEE Intl. Conf. on Mobile Computing and Networking (MobiCom 99), Seattle, WA, August 17-	
	I1	P. Rogaway, M. Bellare, J. Black, and T. Krovetz, "OCB: A block-Cipher Mode of Operations for Efficient Authenticated Encryption," Proc. of the 8th ACM Conf. on Computer	
	J1	S.R. White and L. Comerford, "ABYSS: An Architecture for Software Protection," IEEE Transactions on Software Engineering, vol. 16, No. 6, June 1990, pp. 619-629.	

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.